



Secure Browser Installation Manual

For Technology Coordinators

2014-2015

Published February 10, 2014

Prepared by the American Institutes for Research®



Descriptions of the operation of the Test Information Distribution Engine, Test Delivery System, and related systems are property of the American Institutes for Research (AIR) and are used with the permission of AIR.

Table of Contents

Section I. Introduction to the Secure Browser Manual	1
Scope	1
System Requirements	1
Manual Content	1
Intended Audience	2
Document Conventions	2
Other Resources	3
Section II. Installing the Secure Browser on Desktop and Laptops	4
Installing the Secure Browser on Windows	4
Installing the Secure Browser on an Individual Computer	4
Installing the Secure Browser via Windows	4
Installing the Secure Browser via the Command Line	6
Sharing the Secure Browser over a Network	8
Copying the Secure Browser Installation Directory to Testing Computers	8
Installing the Secure Browser on an NComputing Server	9
Terminal Server Installation	10
Installing the Secure Browser Without Administrator Rights	11
Uninstalling the Secure Browser on Windows	12
Uninstalling via the User Interface	12
Uninstalling via the Command Line	12
Installing the Secure Browser on Mac OS X	13
Installing Secure Browser 7.2	13
Installing Secure Browser 6.5	14
Installing Secure Browser 5.6	15
Uninstalling the Secure Browser on OS X	15
Installing the Secure Browser on Linux	16
Installing the Secure Browser on 32-Bit Distributions	16
Installing the Secure Browser on 64-Bit Distributions	17
Uninstalling the Secure Browser on Linux	17
Section III. Installing the Secure Browser on Mobile Devices	18
Installing the Secure Browser on iOS	18
Installing the Secure Browser on Android	19

Chrome OS AIRSecureTest Kiosk App	21
Installing the AIRSecureTest Kiosk App on Standalone Chromebooks.....	21
Installing the Secure Browser on Windows Mobile Devices.....	24
Section IV. Proxy Settings for Desktop Secure Browsers.....	25
Specifying a Proxy Server to Use with the Secure Browser.....	25
Modifying Desktop Shortcuts to Include Proxy Settings	27
Microsoft Windows	27
Mac OS X	27
Appendix A. Creating Group Policy Objects.....	29
Appendix B. User Support	32

List of Tables

Table 1. Document conventions	2
Table 2. Commands for installing 32-bit compatibility libraries.....	17
Table 3. Specifying proxy settings using a shortcut or the command line	25

Section I. Introduction to the Secure Browser Manual

The secure browser is a web browser for taking online assessments. The secure browser prevents students from accessing other computer or Internet applications and from copying test information. It also occupies the entire computer screen.

Scope

This manual provides instructions for installing the secure browsers on computers and devices used for online assessments.

System Requirements

For the secure browser to work correctly, the computer on which you install it must have a supported operating system. For a list of supported operating systems, see the *System Requirements for Online Testing* available from the Maine Assessment Program portal at <http://me.portal.airast.org>.

Manual Content

This manual is organized as follows:

- [Section I, Introduction to the Secure Browser Manual](#) (this section), describes this guide.
- [Section II, Installing the Secure Browser on Desktop and Laptops](#), includes instructions for installing the secure browser onto supported Windows, Mac, and Linux platforms.
- [Section III, Installing the Secure Browser on Mobile Devices](#), includes instructions for installing the mobile secure browser onto supported iOS, Android, and Chrome OS platforms.
- [Section IV, Proxy Settings for Desktop Secure Browsers](#), provides commands for specifying proxy servers that the secure browser should use.
- [Appendix A, Creating Group Policy Objects](#), describes how to create scripts that launch when a user logs into a Windows computer.
- [Appendix B, User Support](#), provides Help Desk information.

Intended Audience




This installation guide is intended for the following audiences:

- Technology coordinators familiar with downloading installation packages from the Internet or from a network location and installing software onto Windows, Mac OS X, or Linux operating systems or Chromebook, iPad, or Android devices.
- Network administrators familiar with mapping or mounting network drives, and creating and running scripts at the user and host level.
- If you install and run the secure browser from an NComputing server, you should be familiar with operating that software and related hardware.

Document Conventions

[Table 1](#) lists typographical conventions and key symbols.

Table 1. Document conventions

Element	Description
	Warning: This symbol accompanies important information regarding actions that may cause fatal errors.
	Alert: This symbol accompanies important information regarding a task that may cause minor errors.
	Note: This symbol accompanies additional information that may be of interest.
filename	Monospaced text indicates a directory, filename, or something you enter in a field.
text	Bold text indicates a link or button that is clickable.

Other Resources

- For information about technical specifications and related requirements, including supported hardware, software, and text-to-speech, refer to the *System Requirements for Online Testing*.
- For information about securing a computer before a test session, see the *Test Administrator User Guide*.
- For information about network and Internet requirements, general peripheral and software requirements, and configuring text-to-speech settings, see the *Technical Specifications Manual for Online Testing*.

These documents are available at <http://me.portal.airast.org>.

Section II. Installing the Secure Browser on Desktop and Laptops

This section contains installation instructions for Windows and Mac under a variety of deployment scenarios.

Installing the Secure Browser on Windows

This section provides instructions for installing the secure browser on computers running on Windows XP, Vista, 7, 8, and 8.1. (The secure browser does not run on other versions of Windows.)

The instructions in this section assume machines are running a 64-bit version of Windows and that the secure browser will be installed to C:\Program Files (x86)\. If you are running a 32-bit version of Windows, adjust the installation path to C:\Program Files\.

Installing the Secure Browser on an Individual Computer

This section contains instructions for installing the secure browser on individual computers.

Installing the Secure Browser via Windows

In this scenario, a user with administrator rights installs the secure browser using standard Windows. (If you do not have administrator rights, refer to the section [Installing the Secure Browser Without Administrator Rights.](#))


1. If you installed a previous version of the secure browser in a location other than C:\Program Files (x86)\, manually uninstall the secure browser. (If you installed in C:\Program Files (x86)\, the installation package automatically removes it.) See the instructions in the section [Uninstalling the Secure Browser on Windows.](#)
2. Navigate to the **Download Secure Browsers** page of the Maine Assessment Program portal at <http://me.portal.airast.org>. Under **Download Secure Browsers**, click the **Windows** tab, then click **Download Browser**. A dialog window opens.

3. Do one of the following (this step may vary depending on the browser you are using):
 - If presented with a choice to **Run** or **Save** the file, click **Run**. This opens the Secure Browser Setup wizard.
 - If presented only with the option to **Save**, save the file to a convenient location. After saving the file, double-click the installation file MESecureBrowser7.2.msi to open the setup wizard.
4. Follow the instructions in the setup wizard. When prompted for setup type, click **Install**.
5. Click **Finish** to exit the setup wizard. The following items are installed:
 - The secure browser to the default location C:\Program Files (x86)\MESecureBrowser7.2.
 - A shortcut MESecureBrowser7.2 to the desktop.
6. If you are running Windows 8.0 or later do the following (otherwise skip to step 7):
 - a. The Test Policy for AIR setup wizard starts. Click **Continue**.
 - b. Follow the setup wizard, and click **Finish** to exit.

This wizard installs and starts a service Test Policy Standalone Service for Student.

7. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
8. *Optional:* Apply proxy settings by doing the following:
 - a. Right-click the shortcut MESecureBrowser7.2 on the desktop, and select **Properties**.
 - b. Under the **Shortcut** tab, in the **Target** field, modify the command to specify the proxy. See [Table 3](#) for available forms of this command.
 - c. Click **OK** to close the Properties dialog box.

For more information about proxy settings, see [Section IV, Proxy Settings for Desktop Secure Browsers](#).

9. Run the browser by double-clicking the MESecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
10. To exit the browser, click  in the upper-right corner of the screen.

Installing the Secure Browser via the Command Line

In this scenario, a user with administrator rights installs the secure browser from the command line. If you do not have administrator rights, refer to the section [Installing the Secure Browser Without Administrator Rights](#).

1. If you installed a previous version of the secure browser in a location other than C:\Program Files (x86)\, manually uninstall the secure browser. (If you installed in C:\Program Files (x86)\, the installation package automatically removes it.) See the instructions in the section [Uninstalling the Secure Browser on Windows](#).
2. Navigate to the **Download Secure Browsers** page of the Maine Assessment Program portal at <http://me.portal.airast.org>. Under **Download Secure Browsers**, click the **Windows** tab, then click **Download Browser**. A dialog window opens.
3. Save the file on the computer (this step may vary depending on the browser you are using):
 - If presented with a choice to **Run** or **Save** the file, click **Save**, and save the file to a convenient location.
 - If presented only with the option to **Save**, save the file to a convenient location.
4. Note the full path and filename of the downloaded file, such as
c:\temp\MESecureBrowser7.2.msi.
5. Open a command prompt.
6. Run the command `msiexec /I <Source> [/quiet] [INSTALLDIR=<Target>]`

<Source> Path to the installation file, such as C:\temp\MESecureBrowser7.2.msi.

<Target> Path to the location where you want to install the secure browser. If absent, install to C:\Program Files (x86)\MESecureBrowser7.2. The installation program creates the directory if it does not exist.

/I Perform an install.

[/quiet] Quiet mode, no interaction.


For example, the command

```
msiexec /I c:\temp\MESecureBrowser7.2.msi /quiet  
INSTALLDIR=C:\AssessmentTesting\BrowserInstallDirectory
```

installs the secure browser from the installation package at C:\temp\
MESecureBrowser7.2.msi into the directory
C:\AssessmentTesting\BrowserInstallDirectory using quiet mode.

7. Follow the instructions in the setup wizard. When prompted for setup type, click **Install**.
8. Click **Finish** to exit the setup wizard. The following items are installed:
 - The secure browser to the default location C:\Program Files (x86)\MESecureBrowser7.2.
 - A shortcut MESecureBrowser7.2 to the desktop.
9. If you are running Windows 8.0 or later do the following (otherwise skip to step [10](#)):
 - a. The Test Policy for AIR setup wizard starts. Click **Continue**.
 - b. Follow the setup wizard, and click **Finish** to exit.

This wizard installs and starts a service Test Policy Standalone Service for Student.


10. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
11. Run the browser by double-clicking the MESecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
12. To exit the browser, click  in the upper-right corner of the screen.

Sharing the Secure Browser over a Network

In this scenario, you install the secure browser on a server's shared drive, and you also create a shortcut to the secure browser's executable on each testing computer's desktop. This assumes that all testing computers have access to the shared drive.



WARNING Unsupported Installation for Windows 8.x This installation scenario is not supported on test computers running Windows 8.x, and the secure browser does not run. Test computers running Windows 8.x must have local installations as described in [Installing the Secure Browser on an Individual Computer](#).

1. On the remote computer from where the students run the secure browser, install the secure browser following the directions in the section [Installing the Secure Browser on an Individual Computer](#).
2. On each testing machine, sign in and do the following:
 - a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
 - b. Copy the desktop shortcut MESecureBrowser7.2 from the remote machine to the directory C:\Users\Public\Public Desktop.
 - c. Run the browser by double-clicking the MESecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
 - d. To exit the browser, click  in the upper-right corner of the screen.


Copying the Secure Browser Installation Directory to Testing Computers

In this scenario, a network administrator installs the secure browser on one machine, and copies the entire installation directory to testing computers.



WARNING Unsupported Installation for Windows 8.x This installation scenario is not supported on test computers running Windows 8.x, and the secure browser does not run. Test computers running Windows 8.x must have local installations as described in [Installing the Secure Browser on an Individual Computer](#).

1. On the computer from where you will copy the installation directory, install the secure browser following the directions in the section [Installing the Secure Browser on an Individual Computer](#). Note the path of the installation directory, such as C:\Program Files (x86)\MESecureBrowser7.2.

2. Identify the directory on the local testing computers to which you will copy the browser file (it should be the same directory on all computers). For example, you may want to copy the directory to c:\AssessmentTesting\. Ensure you select a directory in which the students can run executables.
3. On each local testing computer, do the following:
 - a. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
 - b. Copy the installation directory C:\Program Files (x86)\MESecureBrowser7.2 from the remote machine to the directory you selected in step 2. For example, if the target directory is c:\AssessmentTesting\, you are creating a new folder c:\AssessmentTesting\MESecureBrowser7.2.
 - c. Copy the shortcut
c:\AssessmentTesting\MESecureBrowser7.2\MESecureBrowser7.2.exe - Shortcut.lnk
to the desktop.
 - d. Run the browser by double-clicking the MESecureBrowser7.2 shortcut on the desktop. The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the task bar.
 - e. To exit the browser, click  in the upper-right corner of the screen.

Installing the Secure Browser on an NComputing Server

In this scenario, a network administrator installs the secure browser on an NComputing server. On testing day, the testing coordinator logs in to the NComputing server from each client and starts the secure browser so that it is ready for the students.

For a listing of supported terminals and servers for this scenario, see the *Technical Specifications Manual for Online Testing*, available from the Maine Assessment Program portal (<http://me.portal.airast.org>).

1. Log in to the machine running the NComputing server.
2. Install the secure browser following the directions in the section [Installing the Secure Browser on an Individual Computer](#).

3. Open Notepad and type or paste the following command:

```
"C:\Program Files (x86)\MESecureBrowser7.2\MESecureBrowser7.2.exe" -CreateProfile  
%SESSIONNAME%
```

4. Save the file as C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\logon.bat.
5. Create a group policy object that runs the file logon.bat each time a user logs in. For details, see [Appendix A, Creating Group Policy Objects](#).
6. Test the installation from a client by doing the following:
 - a. Connect the NComputing server to a terminal, and connect a keyboard and monitor to the same terminal.
 - b. Turn on the monitor, select the NComputing server, and log in. The secure browser's shortcut appears on the desktop.
 - c. Double-click the shortcut to run the secure browser.

Terminal Server Installation

In this scenario, a network administrator installs the secure browser on a terminal server. Testing machines then log in to the terminal server and run the secure browser remotely. This scenario is supported on Windows server 2003 and 2008.



CAUTION: Testing Quality With Terminal Servers Launching a secure browser from a terminal server is typically not a secure test environment, because students can use their local machines to search for answers. Therefore, AIR does not recommend this installation scenario for testing.

1. Log in to the terminal server, and install the secure browser following the directions in the section [Installing the Secure Browser on an Individual Computer](#). Note the path of the installation directory.
2. Copy and paste the line below into Notepad:

```
"C:\Program Files (x86)\MESecureBrowser7.2\MESecureBrowser7.2" -CreateProfile  
%SESSIONNAME%
```

If you used a different installation path, use that in the above command.

3. Save the file as C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\logon.bat.

4. Create a group policy object that runs the file `logon.bat` each time a user logs in. For details, see [Appendix A, Creating Group Policy Objects](#).
5. Modify the MESecureBrowser7.2 desktop shortcut by doing the following:
 - a. Right-click the shortcut and select **Properties**. The Properties dialog box appears.
 - b. Under the **Shortcut** tab, in the **Target** field, type or copy/paste the following command:

```
"C:\Program Files(X86)\MESecureBrowser7.2\MESecureBrowser7.2.exe" -P  
"%SESSIONNAME%"
```
 - c. Click **OK** to close the Properties dialog box.
6. From a different computer, do the following:
 - a. Connect to the terminal server.
 - b. Double-click the desktop shortcut to run the secure browser.

Installing the Secure Browser Without Administrator Rights

In this scenario, you copy the secure browser from one machine where it is installed onto another machine on which you do not have administrator rights.



WARNING Unsupported Installation for Windows 8.x This installation scenario is not supported on test computers running Windows 8.x, and the secure browser does not run. Test computers running Windows 8.x must have local installations as described in [Installing the Secure Browser on an Individual Computer](#).

1. Log on to a machine on which the secure browser is installed.
2. Copy the entire folder where the browser was installed (usually `C:\Program Files (x86)\MESecureBrowser7.2`) to a removable drive or shared network location.
3. Copy the entire directory from the shared location or removable drive to any directory on the target computer.
4. In the folder where you copied the secure browser, right-click `MESecureBrowser7.2.exe` and select **Send To > Desktop (create shortcut)**.

5. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
6. Double-click the desktop shortcut to run the secure browser.

Uninstalling the Secure Browser on Windows

The following sections describe how to uninstall the secure browser from Windows or from the command line.

Uninstalling via the User Interface

The following instructions may vary depending on your version of Windows.

1. Open the Control Panel.
2. Select **Add or Remove Programs** or **Uninstall a Program**.
3. Select the secure browser program MESecureBrowser7.2 and click **Remove** or **Uninstall**.
4. Follow the instructions in the uninstall wizard.

Uninstalling via the Command Line

1. Open a command prompt.
2. Run the command `msiexec /X <Source> /quiet`

`<Source>` Path to the installation file, such as `C:\MSI\MESecureBrowser7.2.exe`.

`/X` Perform an uninstall.

`[/quiet]` Quiet mode, no interaction.

For example, the command

```
msiexec /X C:\AssessmentTesting\MESecureBrowser7.2.exe /quiet
```

uninstalls the secure browser installed at `C:\AssessmentTesting\` using quiet mode.

Installing the Secure Browser on Mac OS X

This section provides instructions for installing the secure browsers on Macintosh desktop computers.

Installing Secure Browser 7.2

In this scenario, a user installs the secure browser on desktop computers running Mac OS X 10.6 through 10.10. The steps in this procedure may vary depending on your version of Mac OS X and your web browser.

1. Remove any previous versions of the secure browser by dragging its folder to the Trash.
2. Navigate to the **Secure Browser** page of the Maine Assessment Program portal at <http://me.portal.airast.org>. Click the **Mac OS X 10.6–10.10** tab, then click **Download Browser**. If prompted for a download location, select your downloads folder.
3. Open Downloads from the Dock, and click MESecureBrowser7.2-OSX.dmg to display its contents.
4. Drag the MESecureBrowser7.2 icon to the desktop.



Note: If a warning message pops up indicating that the secure browser file already exists, select **Replace**.

5. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
6. For Mac OS 10.6 through 10.10, disable Mission Control/Spaces. Instructions for disabling Spaces are in the *Technical Specifications Manual for Online Testing*, available from the Maine Assessment Program portal (<http://me.portal.airast.org>).
7. Double-click the MESecureBrowser7.2 icon on the desktop to launch the secure browser. (You must launch the secure browser to complete the installation.) The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the dock.

**Notes: Possible Warning Messages**

- If a warning message pops up asking if you are sure you want to open the application, click **OK**.
- If a warning message pops up indicating that the secure browser cannot be opened because it is from an unidentified developer, do the following:
 - a) Close the message and open System Preferences.
 - b) Click **Security and Privacy**.
 - c) Click the lock icon to edit settings. If prompted, enter your username and password.
 - d) In the *Allow applications downloaded from* section of the General tab, select **Anywhere**. Confirm your selection.
 - e) If you wish to lock these settings, click the lock icon again.
 - f) Repeat step 7.

Mac OS 10.6: The secure browser disables Exposé (hot corner) settings if they are set, and the settings remain disabled after the browser is closed.



Note: If the secure browser does not fill the entire screen and hide the dock, click **Close** and open it again. If it still does not fill the entire screen and hide the dock, reinstall it and try again.

8. To exit the browser, click **Close** in the upper-right corner of the screen.

Installing Secure Browser 6.5

In this scenario, you install the secure browser on desktop computers running Mac OS 10.5 with an Intel processor. (If your OS 10.5 runs on a Power PC processor, see the section [Installing Secure Browser 5.6](#).)

1. Remove any previous versions of the secure browser by dragging its folder to the Trash.
2. Navigate to the **Secure Browser** page of the Maine Assessment Program portal at <http://me.portal.airast.org>. Click the **Mac OS X 10.5** tab, then click **Download Browser**. A dialog window opens. If prompted for a download location, select the desktop.
3. Open Downloads from the Dock, and click MESecureBrowser6.5-OSX.dmg to display its contents.
4. Drag the MESecureBrowser6.5 icon to the desktop.
5. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.

6. Double-click the MESecureBrowser6.5 icon on the desktop to launch the secure browser. (You must launch the secure browser to complete the installation.) The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the dock.

The secure browser disables Exposé (hot corner) settings if they are set, and the settings remain disabled after the browser is closed.

7. To exit the browser, click **Close** in the upper-right corner of the screen.

Installing Secure Browser 5.6

In this scenario, you install the secure browser on desktop computers running Mac OS 10.5 with a PowerPC processor. (If your OS 10.5 runs on an Intel processor, see the section [Installing Secure Browser 6.5.](#))

1. Remove any previous versions of the secure browser by dragging its folder to the Trash.
2. Navigate to the **Secure Browser** page of the Maine Assessment Program portal at <http://me.portal.airast.org>. Click the **Mac OS X 10.5** tab, then click **Download Browser**. A dialog window opens. If prompted for a download location, select the desktop.
3. If necessary, open the browser's downloads list and click MESecureBrowser5.6-OSX.dmg to display its contents.
4. Drag the MESecureBrowser5.6 icon to the desktop.
5. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
6. Double-click the MESecureBrowser5.6 icon on the desktop to launch the secure browser. (You must launch the secure browser to complete the installation.) The secure browser opens displaying the student login screen. The browser fills the entire screen and hides the dock.
7. To exit the browser, click **Close** in the upper-right corner of the screen.

Uninstalling the Secure Browser on OS X


To uninstall an OS X secure browser, drag its folder to the Trash.

Installing the Secure Browser on Linux

This section provides instructions for installing the secure browser on computers running a supported Linux distribution. For more information about Linux requirements, refer to the *Technical Specifications Manual for Online Testing*, available from the Maine Assessment Program portal (<http://me.portal.airast.org>).

Installing the Secure Browser on 32-Bit Distributions

The instructions in this section are for installing the Linux secure browser onto 32-bit versions of Linux systems. These instructions may vary for your individual Linux distribution.

1. Uninstall any previous versions of the secure browser by deleting the directory containing it.
2. Navigate to the **Secure Browser** page of the Maine Assessment Program portal at <http://me.portal.airast.org>. Click the **Linux** tab, then click **Download Browser**. Save the file to the desktop.
3. Right-click the downloaded file `MESecureBrowser6.5-Linux.tar.bz2`, and select **Extract Here** to expand the file. This creates the `MESecureBrowser6.5` folder on the desktop.
4. In a file manager, open the `MESecureBrowser6.5` folder.
5. Double-click the file `install-icon.sh` and select **Run** from the prompt. The installation program runs and creates a `MESecureBrowser6.5` icon on the desktop.
6. Ensure all background jobs, such as virus scans or software updates, are scheduled outside of test windows. For example, if your testing takes place between 8:00 a.m. and 3:00 p.m., schedule background jobs outside of these hours.
7. If text-to-speech testing is performed on this computer, reboot it.
8. From the desktop, double-click the `MESecureBrowser6.5` icon to launch the browser. The student login screen appears. The browser fills the entire screen and hides any panels or launchers.
9. To exit the browser, click  in the upper-right corner of the screen.

Installing the Secure Browser on 64-Bit Distributions

Use the following procedure to install the secure browser on 64-bit machines.

1. Using [Table 2](#) as a guide, install the 32-bit compatibility libraries for your distribution. If your distribution does not appear in [Table 2](#), consult its documentation for 32-bit compatibility.
2. Install the secure browser by following the procedure in the section [Installing the Secure Browser on 32-Bit Distributions](#).

[Table 2](#) lists the commands for installing 32-bit compatibility libraries for popular Linux distributions.

Table 2. Commands for installing 32-bit compatibility libraries

Distribution	Command
Fedora 16–20	<pre>sudo yum install glibc.i686 sudo yum install nspr.i686 sudo yum install gtk2.i686 sudo yum install xulrunner.i686</pre>
openSUSE 13.1	<pre>zypper install glibc-32bit</pre>
Red Hat Enterprise Linux 6.5	<pre>sudo yum install xulrunner.i686 sudo yum install libgtk-x11-2.0.50.0 sudo yum install libxcom.so sudo yum install glibc.i686</pre>
Ubuntu (LTS) 10.04, 12.04, 14.04	<pre>sudo apt-get install libgtk2.0.0:i386 sudo apt-get install libstdc++6:i386 sudo apt-get install libasound2:i386 libasound2- plugins:i386 sudo apt-get install libdbus-glib-1-2:i386 sudo apt-get install libXt6:i386</pre>

Uninstalling the Secure Browser on Linux

To uninstall a secure browser, delete the directory containing it.

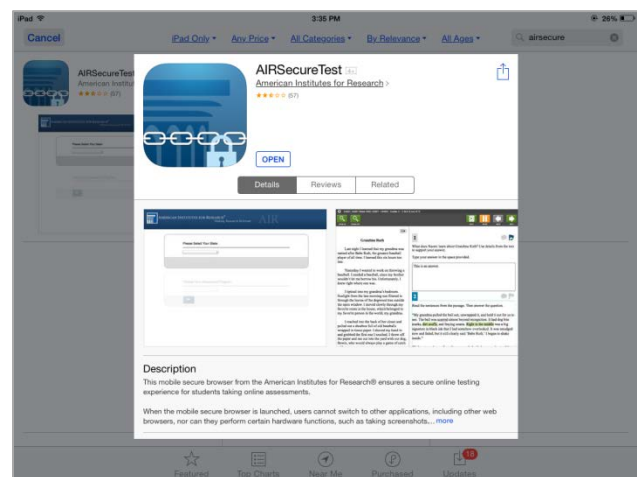
Section III. Installing the Secure Browser on Mobile Devices

This section contains information about installing AIRSecureTest, the secure browser app for iOS, Android, and Chrome OS. For information about configuring supported tablets and Chromebooks to work with the secure browser, refer to the *Technical Specifications Manual for Online Testing*, available from the Maine Assessment Program portal (<http://me.portal.airast.org>).

Installing the Secure Browser on iOS

This section contains instructions for downloading and installing AIRSecureTest and selecting your state and assessment program. The process for installing the secure browser is the same as for any other iOS application.

1. On your iPad, navigate to the **Secure Browser** page of the Maine Assessment Program portal at <http://me.portal.airast.org>, and click the iOS tab. Click **Download**. (You can also search for **AIRSecureTest** in the App store to find the secure browser app.)
2. The AIRSecureTest application download page opens.



3. Tap **Free**. The button changes to **Install App**.



4. Tap **Install App**.



5. Enter your Apple ID password.

The AIRSecureTest mobile secure browser downloads and installs onto your iPad. Look for the AIRSecureTest icon.



The first time you open the AIRSecureTest app, a Launchpad appears. The Launchpad establishes the test administration for your students.

6. Under **Please Select Your State**, select Maine from the drop-down list.



7. Under **Choose Your Assessment Program**, select Maine Assessment Program.
8. Tap or click **OK**. The student login page opens. The secure browser is now ready for students to use.



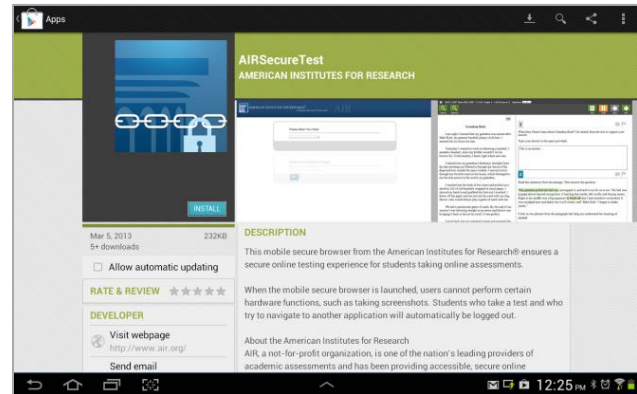
The Launchpad screen appears only once. The student login page appears the next time the secure browser is launched.

Installing the Secure Browser on Android

You can download AIRSecureTest from the Maine Assessment Program portal or from the Google Play store. The process for installing the secure browser is the same as for any other Android application.

This section contains instructions for downloading and installing AIRSecureTest and selecting your state and assessment program.

1. On your Android tablet, navigate to the **Secure Browser** page of the Maine Assessment Program portal at <http://me.portal.airast.org> and tap the Android tab. Click **Download Browser**. (You can also search for “AIRSecureTest” in the Google Play store to find the secure browser app.)
2. The AIRSecureTest application download page appears.



3. Tap **Install**.



4. The AIRSecureTest mobile secure browser downloads and installs onto your tablet. Look for the AIRSecureTest icon. (The name may be truncated.)



Android Secure Browser Keyboard

If the secure browser keyboard has not been selected via device settings on Android tablets, it will need to be selected upon opening the AIRSecureTest app.

For more information about the Android secure browser keyboard, including instructions for enabling it, refer to the *Technical Specifications Manual for Online Testing*, available from the Maine Assessment Program portal (<http://me.portal.airast.org>), Download Secure Browsers page.

The first time you open the AIRSecureTest app, a Launchpad appears. The Launchpad establishes the test administration for your students.

-
- Under **Please Select Your State**, select Maine from the drop-down list.



-
- Under **Choose Your Assessment Program**, select Maine Assessment Program.
 - Tap **OK**. The student login page appears. The secure browser is now ready for students to use.



The Launchpad screen appears only once. The student login page appears the next time the secure browser is launched.



Chrome OS AIRSecureTest Kiosk App

This section contains instructions for installing the AIRSecureTest kiosk application and selecting your state and assessment program.

Installing the AIRSecureTest Kiosk App on Standalone Chromebooks

These instructions are for installing the secure browser on standalone Chromebook devices.

- From your network administrator, obtain the following:
 - The wireless network to which the Chromebook connects. This typically includes the network's SSID, password, and other access credentials.
 - An email and password for logging in to Gmail.
- Power off, then power on your Chromebook.

3. If the OS verification is Off message appears, do the following (otherwise skip to step 4):
 - a. Press the spacebar. In the confirmation screen, press Enter. The Chromebook reboots.
 - b. In the Welcome screen, select your language, keyboard, and the wireless network information you acquired from the network administrator. Back in the Welcome screen, click **Continue**.
 - c. In the Google Chrome OS Terms screen, click **Accept and continue**.
4. When the Sign In screen appears, wipe the Chromebook by doing the following:
 - a. Press Esc +  + Power. The screen displays a yellow exclamation point (!).
 - b. Press Ctrl + D to begin developer mode, then press Enter. The screen displays a red exclamation point.
 - c. Press Ctrl + D, then press Enter. The Chromebook indicates it is transitioning to developer mode. The transition takes approximately 10 minutes, after which the Chromebook reboots.
 - d. After the Chromebook reboots, the OS verification is Off message appears. Press the spacebar, then press Enter. The Chromebook reboots, and the Welcome screen appears.
5. In the Welcome screen, select your language, keyboard, and a network. Back in the Welcome screen, click **Continue**.
6. In the Google Chrome OS Terms screen, click **Accept and continue**. The Sign in screen appears.
7. In the Sign In screen, press Ctrl + Alt + K. The Automatic Kiosk Mode screen appears with a yellow exclamation mark.
8. Click **Enable**, then click **OK**. The Sign in screen appears.
9. In the Sign in screen, enter your email and password, then click **Sign in**.
10. Set your Chromebook preferences as desired.
11. When you get to the desktop, click the Chrome icon () to open Chrome.

12. In the URL bar, enter `chrome://extensions`. The Extensions screen appears.
13. Mark the checkbox for **Developer Mode**.
14. Click **Manage kiosk applications** located at the top of the screen. The Manage Kiosk Applications screen appears.
15. Do the following in the Manage Kiosk Applications screen:
 - a. Enter the following into the **Add kiosk application** field:
`ondcgjblmdblfnmdeoeebaemlckomedj`
 - b. Click **Add**. The **AIRSecureTest** application appears in the Manage Kiosk Applications list.
 - c. Click **Done**. You return to the **Extensions** screen.
16. Click your icon in the lower-right corner and select **Sign Out**.
17. Back at the desktop, click **Apps** at the bottom of the screen, then click **AIRSecureTest**. The secure browser launches.
18. If you receive the following error message, then the secure browser is not configured to run in kiosk mode.

The AIRSecureTest application requires kiosk mode to be enabled.

You need to re-install the app in kiosk mode by following the procedure in this section.


19. The first time you open the AIRSecureTest kiosk app a Launchpad appears. This Launchpad establishes the test administration to which your students will log in. Under **Please Select Your State**, select Maine from the drop-down list.



20. Under **Choose Your Assessment Program**, the Maine Assessment Program should already be selected.

21. Tap or select **OK**. The student login page will load. The secure browser is now ready for students to use.

The Launchpad appears only once. The student login page appears the next time the secure browser is launched.



Installing the Secure Browser on Windows Mobile Devices

The procedure for installing the secure browser on Windows mobile devices is the same for installing it on desktops. See the section [Installing the Secure Browser via Windows](#) for details.

Section IV. Proxy Settings for Desktop Secure Browsers

This section describes the commands for passing proxy settings to the secure browser, as well as how to implement those commands on the desktop computer.

Specifying a Proxy Server to Use with the Secure Browser

By default, the secure browser attempts to detect the settings for your network's web proxy server. You can optionally force the secure browser to use specific proxy settings by passing them through the command line. [Table 3](#) lists the form of the command for different settings and operating systems. To execute these commands from the command line, change to the directory containing the secure browser's executable file.

Table 3. Specifying proxy settings using a shortcut or the command line

Description	System	Command
Run the browser without any proxy	Windows	AIRSecureBrowser7.2.exe -proxy 0
	Mac 10.5 (PPC)	./kiosk-bin ./AIRSecureBrowser5.6 -proxy 0
	Mac 10.5 (Intel)	arch -i386 ./AIRSecureBrowser6.5 -proxy 0
	Mac 10.6–10.10	./AIRSecureBrowser7.2 -proxy 0
	Linux	./AIRSecureBrowser6.5 -proxy 0
Set the proxy for HTTP requests only	Windows	AIRSecureBrowser7.2.exe -proxy 1:http:foo.com:80
	Mac 10.5 (PPC)	./kiosk-bin ./AIRSecureBrowser5.6 -proxy 1:http:foo.com:80
	Mac 10.5 (Intel)	arch -i386 ./AIRSecureBrowser6.5 -proxy 1:http:foo.com:80
	Mac 10.6–10.10	./AIRSecureBrowser7.2 -proxy 1:http:foo.com:80
	Linux	./AIRSecureBrowser6.5.sh -proxy 1:http:foo.com:80

Description	System	Command
Set the proxy for all protocols to mimic the “Use this proxy server for all protocols” of Firefox	Windows	AIRSecureBrowser7.2.exe -proxy 1:*.foo.com:80
	Mac 10.5 (PPC)	./kiosk-bin ./AIRSecureBrowser5.6 -proxy 1:*.foo.com:80
	Mac 10.5 (Intel)	arch -i386 ./AIRSecureBrowser6.5 -proxy 1:*.foo.com:80
	Mac 10.6–10.10	./AIRSecureBrowser7.2 -proxy 1:*.foo.com:80
	Linux	./AIRSecureBrowser6.5.sh -proxy 1:*.foo.com:80
Specify the URL of the PAC file	Windows	AIRSecureBrowser7.2.exe -proxy 2:proxy.com
	Mac 10.5 (PPC)	./kiosk-bin ./AIRSecureBrowser5.6 -proxy 2:proxy.com
	Mac 10.5 (Intel)	arch -i386 ./AIRSecureBrowser6.5 -proxy 2:proxy.com
	Mac 10.6–10.10	./AIRSecureBrowser7.2 -proxy 2:proxy.com
	Linux	./AIRSecureBrowser6.5.sh -proxy 2:proxy.com
Auto-detect proxy settings	Windows	AIRSecureBrowser7.2.exe -proxy 4
	Mac 10.5 (PPC)	./kiosk-bin ./AIRSecureBrowser5.6 -proxy 4
	Mac 10.5 (Intel)	arch -i386 ./AIRSecureBrowser6.5 -proxy 4
	Mac 10.6–10.10	./AIRSecureBrowser7.2 -proxy 4
	Linux	./AIRSecureBrowser6.5.sh -proxy 4
Use the system proxy setting (default)	Windows	AIRSecureBrowser7.2.exe -proxy 5
	Mac 10.5 (PPC)	./kiosk-bin ./AIRSecureBrowser5.6 -proxy 5
	Mac 10.5 (Intel)	arch -i386 ./AIRSecureBrowser6.5 -proxy 5
	Mac 10.6–10.10	./AIRSecureBrowser7.2 -proxy 5
	Linux	./AIRSecureBrowser6.5.sh -proxy 5

Modifying Desktop Shortcuts to Include Proxy Settings

This section provides guidelines for passing a proxy setting to the secure browser. All commands in this section are examples only, with the assumption that you have a shortcut for the secure browser on your desktop.

Microsoft Windows

1. Right-click the desktop shortcut for the secure browser, and select **Properties**.
2. Under the Shortcut tab, in the **Target** field, modify the command as specified in [Table 3](#). For example:

```
"C:\Program Files (x86)\AIRSecureBrowser7.2\AIRSecureBrowser7.2.exe" -proxy  
1:http:foo.com:80
```

3. Click **OK**.

Mac OS X

The steps in this section require you to use Terminal and a text editor.

1. Open the terminal by selecting **Applications > Utilities > Terminal**.
2. Change to the desktop directory

```
cd Desktop
```

3. Create a file `securebrowser.command` on the desktop using a text editor such as Pico.

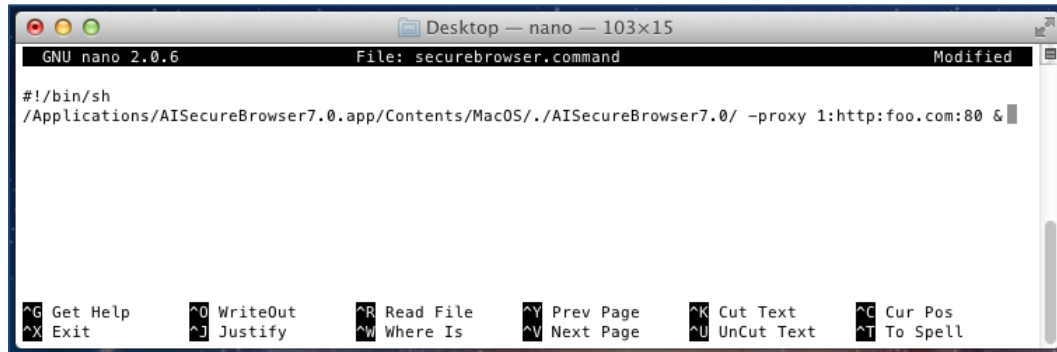
```
pico securebrowser.command.
```

4. Copy or type the following the lines:

```
#!/bin/sh  
/Applications/AIRSecureBrowser7.2.app/Contents/MacOS/./  
AIRSecureBrowser7.2 -proxy 1:http:foo.com:80 &
```

Be sure to specify the complete path to the secure browser and the desired proxy option. Ensure the command ends with an ampersand &. For example, for Mac 10.6–10.10:

Figure 1. Sample Mac 10.7.5 Command



```
GNU nano 2.0.6      File: securebrowser.command      Modified
#!/bin/sh
/Applications/AISecureBrowser7.0.app/Contents/MacOS/./AISecureBrowser7.0/ -proxy 1:http:foo.com:80 &

^G Get Help      ^O WriteOut      ^R Read File      ^V Prev Page      ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^N Next Page     ^U UnCut Text    ^T To Spell
```

5. Save the file and exit the editor by pressing **Ctrl-O**, **Enter** and **Ctrl-X**.
6. Apply execute permission to the file. In Terminal, type

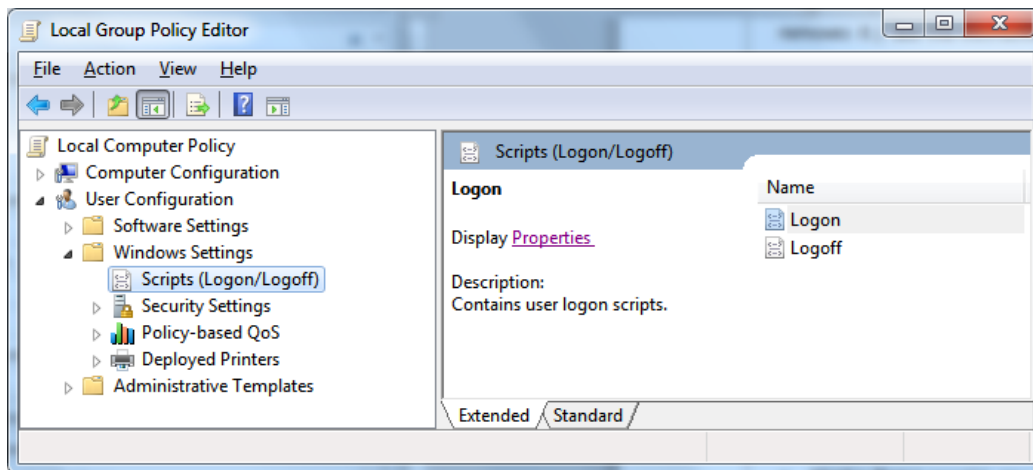
`chmod a+x securebrowser.command`
7. Close Terminal.
8. Click the `securebrowser.command` icon on the desktop. The secure browser opens with the proxy setting you configured.

Appendix A. Creating Group Policy Objects

Many of the procedures in the section [Installing the Secure Browser on Windows](#) refer to creating a group policy object. These are objects that Windows executes upon certain events. The following procedure explains how to create a group policy object that runs a script when a user logs in. The script itself is saved in a file `logon.bat`.

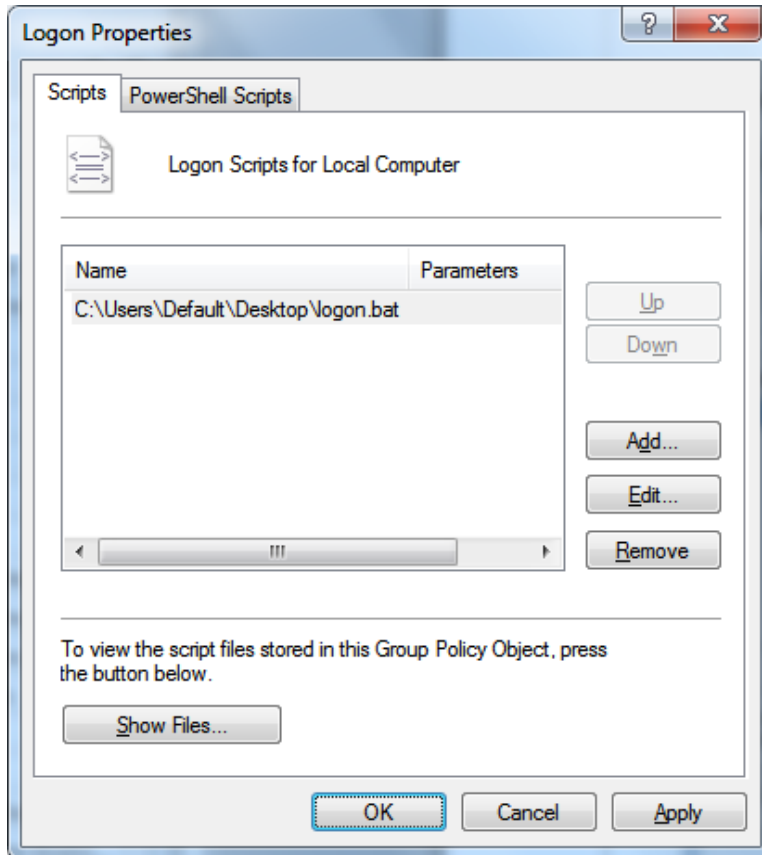
For additional information about creating group policy objects, see “Assign user logon scripts” at <http://technet.microsoft.com/en-us/library/cc781361%28v=ws.10%29.aspx>.

1. **Start > Run > gpedit.msc.** The Local Group Policy Editor appears.

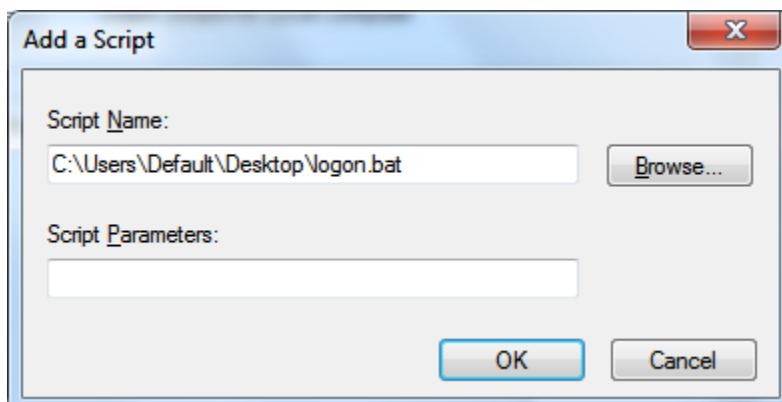


2. Expand **Local Computer Policy > User Configuration > Windows Settings > Scripts (Logon/Logoff).**

3. Select **Logon** and click **Properties**. The Logon Properties dialog box appears.



4. Click **Add**. The Add a Script dialog box appears.



5. Click **Browse...**, and navigate to the logon.bat you want to run.
6. Click **OK**. You return to the Logon Properties dialog box.

7. Click **OK**. You return to the Local Group Policy Editor.
8. Close the Local Group Policy Editor.

Appendix B. User Support

If this document does not answer your questions, please contact the Maine Assessment Program Help Desk.

The Help Desk will be open Monday–Friday from 7:00 a.m. to 7:00 p.m. Eastern Time during the summative testing window and 8:00 a.m. to 5:00 p.m. Eastern Time outside of the summative testing window (except holidays).

Maine Assessment Program Help Desk

Toll-Free Phone Support: 1-844-560-7814

Email Support: mehelpdesk@air.org

If you contact the Help Desk, you will be asked to provide as much detail as possible about the issues you encountered.

Include the following information:

- Test Administrator name and IT/network contact person and contact information
- SSIDs of affected students
- Results ID for the affected student tests
- Operating system and browser version information
- Any error messages and codes that appeared, if applicable
- Information about your network configuration:
 - Secure browser installation (to individual machines or network)
 - Wired or wireless Internet network setup